NASA TECH BRIEF
*Ames Research Center*



# Digital Random-Number Generator

## The problem:

To generate random numbers within a digital computer system in minimum time. Random numbers are ordinarily generated in digital computers by slow software programs which require card decks or tapes; in some computers, the outputs of analog noise generators are sampled by analog-to-digital conversion systems which are slow and require use of sampling channels that already are at a premium.

## The solution:

For a binary digit array of N bits, use N noise sources to feed N nonlinear operators; each flip-flop in the digit array is set by a nonlinear operator to reflect whether the amplitude of the generator which feeds it is above or below the mean value of the generated noise.

## How it's done:

The noise generators are provided with very high frequency noise of stationary statistics (not time varying) by independent noise sources such as cascade diodes, noise vacuum tubes, etc. No prior knowledge of the envelope of the noise statistics is required except for location of the statistical mean.

The switch point of the nonlinear operators receiving outputs from noise generators are centered at the statistical mean values of the noise for each generator; thus, the output of a given nonlinear operator will have a voltage value corresponding either to the "zero" level or the "one" level of the flip-flop to which it is connected in the register of N digits (the word length required by the computer). Since the noise from a generator fluctuates randomly about its statistical mean, the output from the nonlinear operator which is fed by the generator will be randomly "zero" or "one;" thus, each bit in the register array is generated randomly, and the binary digital number represented by the register at any given instant will be random.

Numbers generated in this fashion have a discrete distribution which is uniformly distributed over the interval of zero to 2 exp(N—1). The spacing between points on the distribution is ½ exp(N—1) corresponding to the step of the least significant bit in the digital word (bit N); the probability of any one point occurring is ½ exp(N).

The binary word format adopted here is natural binary. Translations between this and any other format (e.g., floating point) can be easily accomplished by logical control into or out of the binary word register. Control and timing of word transfers into the digital computer are a function of the interface logic required by the exchange module of the specific digital computer selected.

## Notes:

1. The fixed-point uniform distribution random number generation method can also be used to generate random numbers with a distribution other than uniform, for example, Gaussian.
2. No other documentation is available. Specific questions, however, may be directed to:

   Technology Utilization Officer
   Ames Research Center
   Moffett Field, California 94035
   Reference: B73-10266

(continued overleaf)

**Patent status:**

Inquiries concerning rights for the commercial use of this invention should be addressed to:

NASA Patent Counsel
Mail Code 200-11A
Ames Research Center
Moffett Field, California 94035

Source: David H. Brocker
Ames Research Center
(ARC-10096)